DOI: 10.25586/RNU.V9187.20.02.P.146 УДК 004.056.53

Г.И. Спиридонов

ИССЛЕДОВАНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Исследуются и анализируются основные виды угроз безопасности информации, а также наиболее распространенные виды утечек информации.
Ключевые слова: информационная безопасность, безопасность информационных технологий, информационные системы, каналы утечки информации, несанкционированный доступ.

G.I. Spiridonov

RESEARCH OF LEAKAGE CHANNELS AND UNAUTHORIZED ACCESS

The main types of threats to information security, as well as the most common types of information leaks, are investigated and analyzed.
Keywords: information security, information technology security, information systems, prospective methods of information security, information leakage, unauthorized access.

Классификация всех возможных угроз информационной безопасности автоматизированной системы (АС) может быть проведена по ряду признаков (рис. 1) [2].

В зависимости от рассматриваемой предметной области в каждом конкретном случае классификация может быть дополнена. Рассмотрим классификацию угроз информационной безопасности по базовым признакам.

- по природе возникновения;
- степени преднамеренности проявления;
- непосредственному источнику угроз;
- положению источника угроз;
- степени зависимости от активности АС;
- степени воздействия на АС;
- способу доступа к ресурсам АС;
- текущему месту расположения информации, хранимой и обрабатываемой в АС.

Независимо от определения конкретного вида или класса угроз система защиты информации должна удовлетворять требованиям тех лиц, которые ее эксплуатируют, должна обеспечивать общие свойства информации и систем ее обработки.

Исследование угроз безопасности информации позволило классифицировать уязвимость компонентов распределенной вычислительной системы (рис. 2), наиболее подверженных атакам [Там же].

Для создания защищенной информационной системы необходимо определить, на каком из этапов возможно проявление того или иного изъяна защиты, т.е. источника появления той или иной уязвимости.

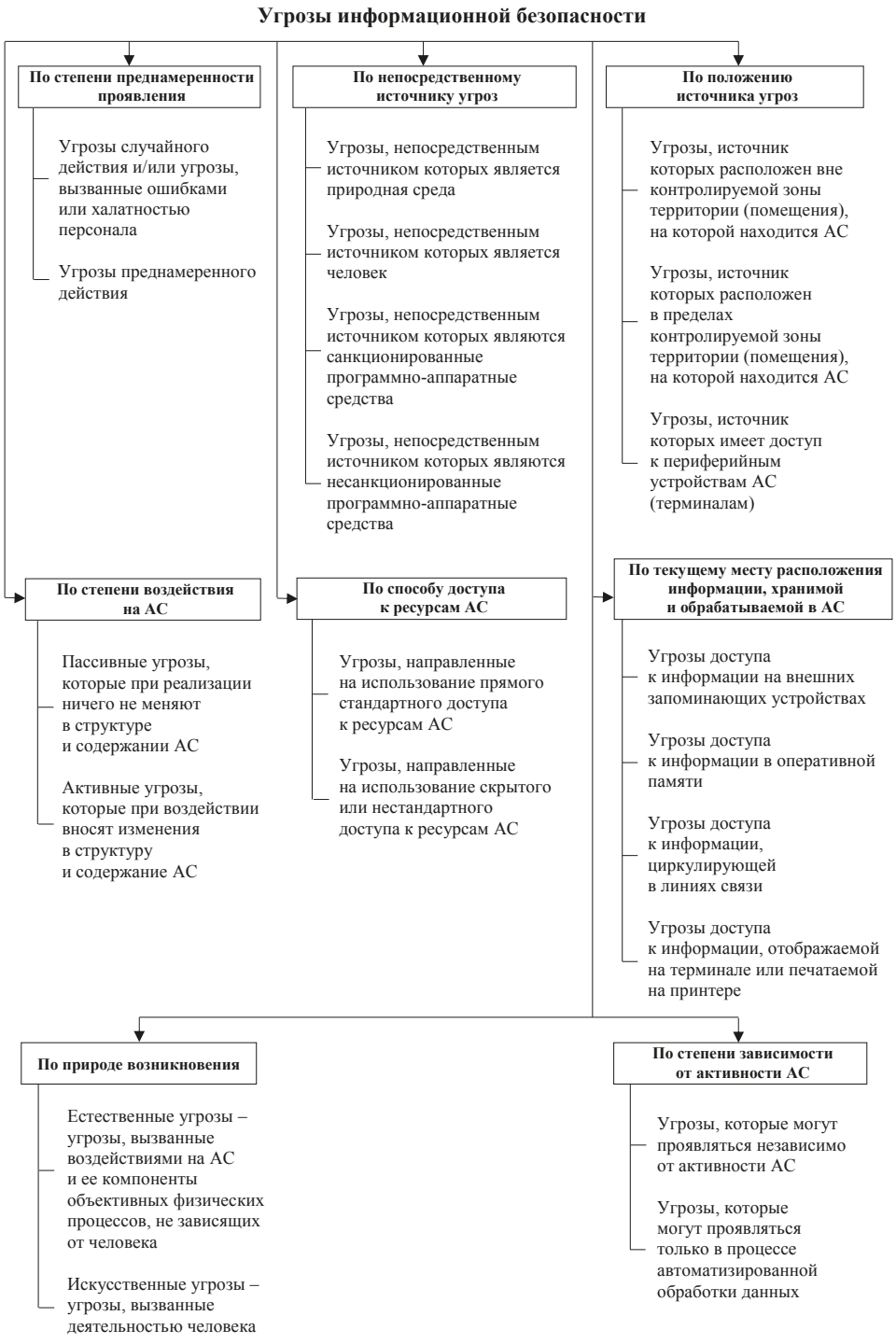

Рис. 1. Классификация угроз информационной безопасности

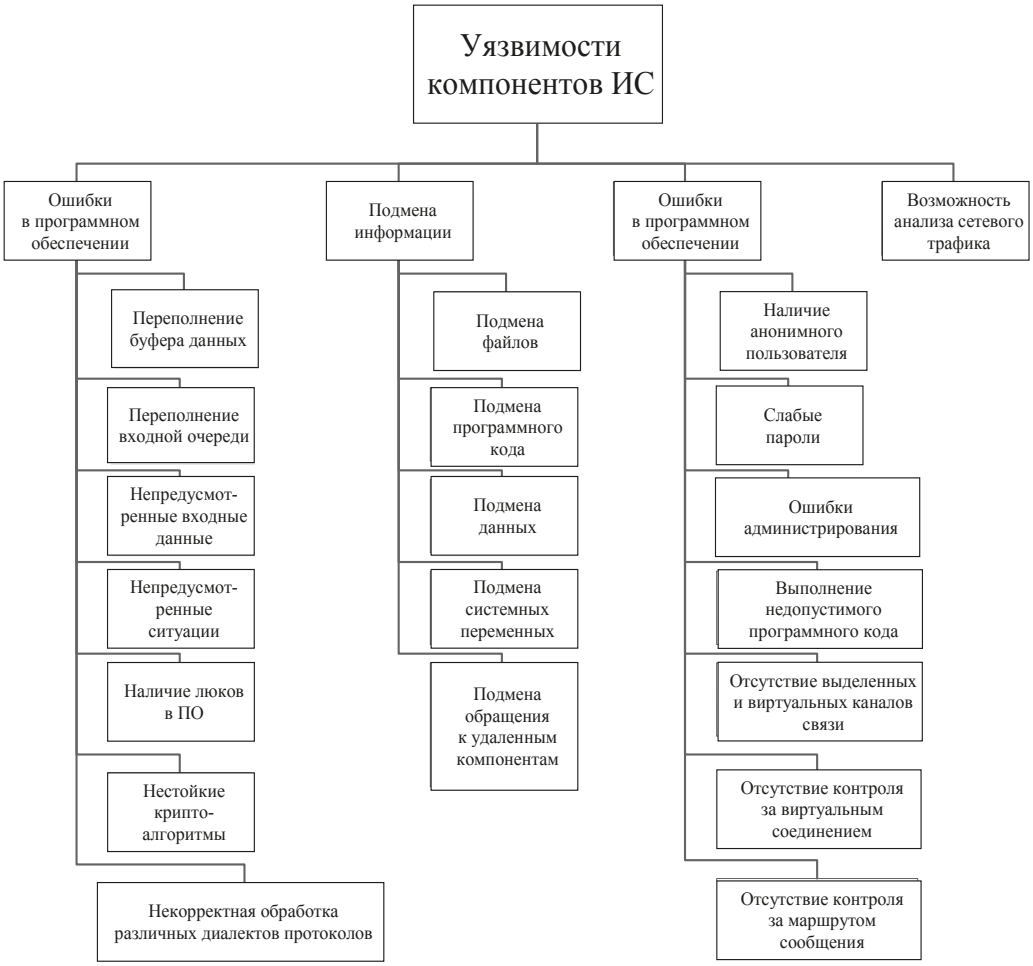

Рис. 2. Классификация уязвимостей компонентов информационных систем

Сопоставление уязвимостей компонентов распределенной вычислительной системы и ошибок, допущенных на различных этапах ее создания, приведено на рисунке 3.

Анализ уязвимостей компонентов распределенной вычислительной системы и методов защиты позволил сделать следующие выводы [1].

1. Источники появления изъянов защиты в основном связаны с неправильным применением и внедрением моделей безопасности, целостности и работоспособности.

2. Большое количество атак связано с нарушением конфиденциальности информации.

На основании проведенного компанией InfoWatch исследования утечек можно выделить следующие наиболее актуальные каналы утечки информации.

В 2019 г. аналитическим центром InfoWatch зарегистрировано 1276 (3,5 в день, 106,3 в месяц) случаев утечки конфиденциальной информации (рис. 4). Это на 22,8% больше, чем в 2018 г. (1039 утечки).

Рис. 3. Сопоставление уязвимостей компонентов вычислительной системы и ошибок, допущенных на различных этапах ее создания

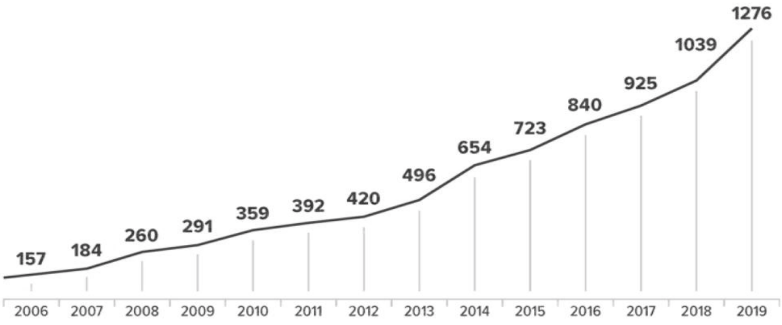

Рис. 4. Общее число обнаруженных утечек информации, 2006–2019 гг., ед.

По результатам исследования ясно, что все чаще появляются утечки, которые ранее были неизвестными. К таким утечкам можно отнести компрометацию больших объемов данных, связанных с платежами или кредитными картами, утечки информации из государственных предприятий или крупных предприятий с мировыми именами [6].

В 2019 г. распределение утечек между случайными и умышленными изменилось в сторону случайных примерно на 8%, доля умышленных наоборот снизилась примерно на 2% (рис. 5).

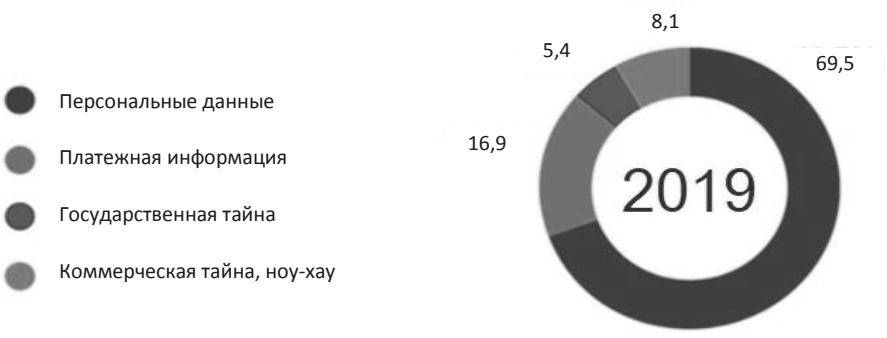

Рис. 5. Диаграммы распределения видов утечек информации, 2019 г., %

Резкое увеличение числа утечек персональных данных (см. рис. 5) в России связано с развитием сервисов, которые обрабатывают персональные данные, и соответственным увеличением объемов обрабатываемых данных. В большинстве случаев утечка информации происходила по вине внутреннего нарушителя. Речь идет о краже данных бывшими и настоящими сотрудниками компаний, а также подрядчиками. Незначительной остается и доля утечек, связанных с использованием смартфонов и других мобильных устройств.

При исследовании утечек с помощью съемных носителей выявлено, что в данном случае доля умышленных утечек меньше, чем неумышленных, однако ущерб, причиняемый организациям в результате таких утечек, может быть значительным, так как такие утечки связаны, как правило, с очень дорогостоящей или значимой для предприятия информацией.

Главными инструментами противодействия угрозам несанкционированного доступа являются организационно-правовые методы и физические средства защиты информации. Организационные меры по обеспечению информационной безопасности являются основной всех мероприятий по построению системы защиты информации. От того, насколько полно и качественно руководством предприятия построена организационная работа по защите информации, зависит эффективность системы защиты информации в целом, так как правильная постановка задачи на обеспечение мер по защите информации и грамотное распределение обязанностей между исполнителями – это фундамент построения любой системы [6; 7].

Место и роль организационных мероприятий в общей системе используемых методов защиты конфиденциальной информации предприятия определяются важностью принятия топ-менеджментом своевременных и взвешенных решений на основании текущей ситуации с защитой информации, в том числе в результате анализа имеющихся в распоряжении предприятия методов и средств обеспечения информационной безопасности с использованием текущего пакета законодательных актов.

Грамотная реализация политики информационной безопасности современного предприятия предполагает применение комплексного подхода [4; 5].

Системы парольной защиты часто подвергаются атакам со стороны злоумышленников. Выбор адекватных мер противодействия во многом зависит от понимания природы существующих угроз. Общедоступное программное обеспечение, используемое в локальных вычислительных сетях, не обеспечивает надежного разграничения доступа и позволяет злоумышленнику легко вскрывать эту систему. Стойкость системы определяется ее способностью противостоять атаке злоумышленника, завладевшего базой данных учетных записей и пытающихся восстановить пароли.

Все физические средства защиты основаны на взаимосвязанном применении различных механических, электронных или электромеханических приспособлений, которые созданы специально для создания препятствий различного рода на возможных путях несанкционированного проникновения нарушителей к самой системе или ее компонентам. Сюда относят и средства видеонаблюдения и охранную сигнализацию.

Аппаратно-программные (технические) меры для защиты обычно создаются на основе различных электронных устройств в совокупности со специальными программами, выполняющими (самостоятельно или в связке с другими похожими средствами) функции защиты, такие как аутентификацию и идентификацию каждого пользователя, разграничение доступа, запись всех событий в системе, шифрование данных и т.п. (ГОСТ Э 51241–2008) [8].

Для предотвращения нелегального доступа посторонних лиц к данным и информации нужно обеспечить надежные механизмы распознавания каждого пользователя (или отдельных групп). Для этого могут применяться различные приспособления: ключи, магнитные карты, дискеты и т.д.

Однако ЛВС компаний развивается, увеличивается количество ее элементов, а вместе с ней увеличивается и количество возможных уязвимостей сети, на которые может быть совершена атака как изнутри (недобросовестными сотрудниками компании), так и снаружи – лицами, заинтересованными в несанкционированном доступе к информации (конкурентами, преступными организациями).

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

В связи с этим существует необходимость в создании комплексной системы обеспечения информационной безопасности утечек от несанкционированного доступа [3; 9].

Литература

1. *Адаменко М.А.* Основы классической криптологии. Секреты шифров и кодов. М.: ДМК Пресс, 2012. 256 с.

2. *Бирюков А.А.* Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.

3. *Гладышев А.И., Аборкина Е.С.* Вопросы применения существующих методов оценки сложности информационных систем // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ, управление». 2016. Вып. 1–2. С. 114–118.

4. ГОСТ Р 51275–2006. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М., 2007. 7 с.

5. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № Пр-646. М., 2016. 16 с.

6. Информационная безопасность в корпоративном секторе. URL: http://info-watch.ru (дата обращения: 06.05.2020).

7. *Платонов В.* Программно-аппаратные средства защиты информации: учебник. М.: Academia, 2014. 336 с.
8. *Родичев Ю.А.* Нормативная база и стандарты в области информационной безопасности: учебное пособие. СПб.: Питер, 2017. 256 с.
9. *Семененко В.А.* Информационная безопасность: учебное пособие. 4-е изд., стер. М.: МГИУ, 2010. 277 с.

Literatura

1. *Adamenko M.A.* Osnovy klassicheskoj kriptologii. Sekrety shifrov i kodov. M.: DMK Press, 2012. 256 s.
2. *Biryukov A.A.* Informatsionnaya bezopasnost': zashchita i napadenie. M.: DMK Press, 2012. 474 s.
3. *Gladyshev A.I., Aborkina E.S.* Voprosy primeneniya sushchestvuyushchikh metodov otsenki slozhnosti informatsionnykh sistem // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz, upravlenie". 2016. Vyp. 1–2. S. 114–118.
4. GOST R 51275–2006. Ob"ekt informatizatsii. Faktory, vozdejstvuyushchie na informatsiyu. Obshchie polozheniya. M., 2007. 7 s.
5. Doktrina informatsionnoj bezopasnosti Rossijskoj Federatsii ot 5 dekabrya 2016 g. № Pr-646. M., 2016. 16 s.
6. Informatsionnaya bezopasnost' v korporativnom sektore. URL: http://infowatch.ru (data obrashcheniya: 06.05.2020).
7. *Platonov V.* Programmno-apparatnye sredstva zashchity informatsii: uchebnic. M.: Academia, 2014. 336 s.
8. *Rodichev Yu.A.* Normativnaya baza i standarty v oblasti informatsionnoj bezopasnosti: uchebnoe posobie. SPb. :Piter, 2017. 256 s.
9. *Semenenko V.A.* Informatsionnaya bezopasnost': uchebnoe posobie. 4-e izd., ster. M.: MGIU, 2010. 277 s.

DOI: 10.25586/RNU.V9187.20.02.P.152 УДК 004.052.42+004.056.53

О.Ю. Жарова

РАЗРАБОТКА ИЕРАРХИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ ВНЕШНЕГО ВОЗДЕЙСТВИЯ ДЕСТРУКТИВНЫХ ПОТОКОВ ДАННЫХ НА ТЕХНОЛОГИЧЕСКУЮ СЕТЬ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Цель исследования заключается в разработке инструментария прогнозирования и минимизации возможного ущерба от деструктивных потоков данных, направленных на технологические сети промышленных предприятий. На основе анализа приведены статистические данные, демонстрирующие актуальность проблемы кибератак, направленных на технологические сети промышленных предприятий по всему миру. Описан первый инцидент и последующая динамика нарастания кибердавления. Сделан вывод о причине медленной реакции на инциденты со стороны предприятий. Рассмотрена проблема деструктивных потоков данных в технологических сетях и приведены результаты научно-исследовательской работы, направленной на противодействие им. Приведена и подробно описана разработанная иерархическая модель.

Ключевые слова: технологические сети, киберугроза, DoS/DDoS-атака, внешнее воздействие деструктивных потоков данных, иерархическая модель, статистические параметры трафика.